

IN THE SPECIFICATION

Please replace the paragraph beginning on page 1, line 10, with the following replacement paragraph:

Most security arrangements rely heavily on the use of public-key cryptography, X.509 certificates and public-key infrastructure (PKI) to provide scalability. Critical to such security arrangements is that each end user and user device can be authenticated by an X.509 certificate. However, this assumption may not be viable for future systems because there are serious key management issues relating to PKI design and deployment. Indeed, there is no real cost effective solution for certificate revocation and key management. Secret-key cryptography, where communicating parties must share a security key in advance, e.g., ID/Password, will continue to play an important role for user authentication in an enterprise or public communication environment. Although secret-key arrangements are simple and highly portable, they are not scalable.